Before the

Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	))	WT Docket No. 06-150
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)))	PS Docket No. 06-229
	)	
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100

COMMENTS OF LAYER 2 CONNECTIONS, LLC

Layer 2 Connections, LLC ("Layer 2 Connections") hereby submits the following comments in response to the Commission's Third Report and Order and Fourth Further Notice of Proposed Rulemaking, released January 26, 2011.

EXECUTIVE SUMMARY

Layer 2 Connections advocates that there are several important areas that the FCC should consider in its rulemaking:

- There is a need for rules that address the transition from commercial and private networks used by public safety agencies today to emerging 700 MHz Public Safety networks. In some cases we believe that public safety agencies may need to support both legacy and 700 MHz systems, operated by different identity and authorization authorities, long after the 700 MHz system build is complete in order to enhance coverage, capacity and resilience-through-diversity.

- In emergency situations public safety agencies may need to extend the coverage and capacity of their communications networks while also delivering more resilience. We anticipate that these agencies will want failover between available networks to be seamless to all applications and services and when additional capacity is required that any combination of available networks can bonded together and used simultaneously for all application or service they may require to use. We note that providing these capabilities will result in maximum spectrum utilization for the FCC and maximum safety and flexibility for public safety agencies.

- Regardless of whether a single network or "network-of networks" approach is taken for the 700 MHz Public Safety Network we anticipate that a variety of legacy networks will need to be supported by public safety agencies. This suggests to us that applications and services need to be provided with quality of service capabilities that are network agnostic placing public safety agencies in full control of how current and future networks are used for what purpose and by whom.

As such, Layer 2 Connections makes 3 specific requests of the FCC for consideration in rulemaking that we believe are in the public's interest of improving the safety and productivity of our nation's first responders:

1) The FCC should extend the concept of the "network of networks" from referring to the combination of all Regional and Tribal 700 MHz Public Safety Networks to encompass networks of all types – regardless of mode or band.

RATIONALE: This broader approach will maximize the chances that a public safety agency is able to benefit from using whatever connectivity is available and allow the FCC to maximize use of spectrum resources. This connectivity may also include unregulated free and available WiFi in proximity of the responder.

2) The FCC define and mandate that roaming handoff – whether intra-system or inter-system – be defined explicitly as requiring a "Make-Before-Break" seamless transition. We consider a handoff as "Make-Before-Break" when a viable path is established across a secondary network (or multiple secondary networks) before a primary network is dropped. Establishing viability for roaming requires that a network's available bandwidth, packet loss, latency and jitter are taken into consideration prior to the handoff. Without establishing such metrics, handoff between networks will be best-efforts rather than best-quality leading to unexpected and unwanted outcomes. We believe that the measurement and reporting of the metrics should not rely on the cooperation of the network operator – that is: public safety agencies should be able to establish the performance metrics of a network regardless of whether the operator of that network is cooperative or uncooperative in making this information available.

RATIONALE:

A. First responders who roam a data session between disparate LTE networks and/or between an LTE network and something-other-than an LTE network must be able to maintain continuity of session, with no noticeable break – especially for real-time protocols like Voice-over-IP (VoIP) and Video. If a break were to occur during handoff (such as with a "break-before-make" handoff), the situational awareness of the first responder, and hence their safety and productivity, can be hampered.

B. Legacy commercial and private networks are needed to provide both support for transition/migration to the 700 MHz Public Safety Broadband Network and resilience/backup in case of future outage or congestion of the 700 MHz Public Safety Broadband Network. "Make-before-break" Seamless Handoff is required to fully leverage key applications that support first responder situational awareness, and affects both intra-system roaming and inter-system roaming.

C. Enabling ubiquitous in-building coverage for The Public Safety Broadband Network is likely to be years away and cost prohibitive. As many buildings already have WiFi installations, a "Make-Before-Break" Seamless Handoff between the 700MHz Public Safety Broadband Network and available Wi-Fi networks can help first responders to maintain connectivity, and hence situational awareness, while outside of coverage of the 700 MHz Public Safety Broadband Network.

3) The FCC mandate that the capability of Network Bearer Bonding – enabling the combined bandwidth of multiple similar and/or dissimilar networks to be utilized for the same data session simultaneously –improving resilience and providing additional capacity outside of the 700 MHz Public Safety Broadband Network.

RATIONALE: Network Bearer Bonding can boost the network capacity available to a first responder in the field, allowing improved situational awareness and hence improved safety and productivity. While it is understood that significant nodes in the 700 MHz Public Safety Broadband Network will have increased resilience and hardening built in, there remain many single points of failure in it. During times of outage and congestion, bearer bonding can increase the likelihood that first responders remain able to communicate with adequate bandwidth. Bearer bonding also supports public and private partnership, by enabling cooperation between commercial carriers and the public safety community to ultimately make first responders safer and more productive.

Our detailed response to sections of the FCC Requests for Comment follows below.

DETAILED SECTION RESPONSES

This portion of Layer 2 Connections' commentary extracts specific sections of the Commission's Third Report and Order and Fourth Further Notice of Proposed Rulemaking, and provides specific comments. Unless otherwise cited, all extracts are directly quoted from the FCC's Third Report and Order and Fourth Further Notice of Proposed Rulemaking.

EXTRACT – SECTIONS 7 AND 8

7. In the *Second Report and Order*, we [the FCC] mandated that the shared network incorporate, among other technical specifications, "a broadband technology platform that provides mobile voice, video and data capability that is seamlessly interoperable across agencies, jurisdictions and geographic areas" and that also includes "current and evolving state-of-the-art technologies reasonably made available in the commercial marketplace with features beneficial to the public safety community (*e.g.*, increased bandwidth)."[1] We reiterated this baseline requirement in the *Third Further Notice*, where we tentatively concluded that "the shared

[1] *Third Further Notice* at 14336-37 ¶ 95.

wireless broadband network must provide for fixed and mobile voice, video and data capability"[2] and that the network "must use a common air interface."[3]

8. There is substantial support for our proposal to require use of a common air interface on the public safety network. US Cellular, for example, states that "an interoperable network of networks providing advanced public safety applications requires a common air interface,"[17] while NPSTC contends that "[v]arying technology platforms [would] present challenges to efficient and effective interoperability."

LAYER 2 COMMENTS -- SECTIONS 7 AND 8

The above comments describe interoperability at Layer 1 (the physical layer) of the Open System Interconnect (OSI) model. Interoperability can also be achieved at higher layers – such as Layer 2 (Link) and Layer 3 (Network). Using Layer 2 tunneling across various wide area networks that would normally be considered to be disparate can make them perform as if they were one single broadcast domain. This is called Wide Area Network Virtualization.

EXTRACT – SECTION 10

10. While we [the FCC] continue to believe in the importance of technological neutrality as a policy, we believe that, in the instant case, establishing a common air interface for 700 MHz public safety networks is necessary to achieve our critical goal of a nationwide interoperable public safety wireless broadband network.

…In the Fourth Further Notice below, we seek comment on how to address the use of future technology platforms that may arise to ensure that they are interoperable and backward compatible with the LTE requirements designated in this Third Report and Order or in subsequent orders.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 10

While Layer 2 Connections agrees with the statement that "a common air interface for 700 MHz public safety networks is necessary to achieve our critical goal...," we also acknowledge that if the physical 700 MHz public safety network is rendered inoperative, this creates a single point of

[2] *Id*. at 14340 ¶ 106.
[3] *Id*. at 14342 ¶ 110.

failure. Interoperability can be created using a network of networks in a manner that allows other air interfaces to supplement and replace the 700 MHz Public Safety Network should it become congested or unavailable.

EXTRACT – SECTION 15 (including reference 37)

15. This Fourth Further Notice addresses interoperability from a technological perspective. It considers interoperability at various communication layers, namely the physical layer, network layer and application layer.

Reference 37 - The concept of layering that first introduced by ISO provides OSI layers consisting of seven layers of functional capabilities within each device or network node. The follow up developments in the industry produced lower number of layers, and in fact, based on needed requirements, various organizations introduced various number of layers based on their needs. We selected 3 layers for practical reasons. Layer 2 of OSI is collapsed into Layer 1 and dubbed as the Physical layer, Layer 3 stays intact as being the Network layer, and Layers 4, 5 and 6 all merge into layer 7, the Application layer.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 15

Layer 2 Connections believes that collapsing Layer 1 (Physical) and Layer 2 (Data-Link) limits the options of placing network endpoints on different physical networks and at the same time allowing them to participate as part of the same broadcast domain using Virtual Local Area Networks (VLAN). We note that if common broadcast domains can be extended to remote nodes regardless of the physical network (or networks) to which they are attached then mission-critical services such as one-to-one and one-to-many voice and video communications can be delivered far more effectively and efficiently.

EXTRACT – SECTION 16

As an initial matter, we seek comment on the definition of "interoperability" for purposes of the public safety broadband network in the 700 MHz band. Part 90 of Commission rules defines interoperability as "an essential communication link within public safety and public service wireless communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results.4 The Department of Homeland Security (DHS) Office of Interoperability and Compatibility (OIC), however, defines interoperability as "the ability of public safety agencies to talk to one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."5 We propose to amend the Commission's definition of interoperability in Part 90 to harmonize it with DHS's because we believe that the broader definition is the true definition of interoperability we seek to achieve (i.e., ensuring that the public safety community, whoever and wherever they are, is able to communicate with one another). We seek comment on our proposal. Interoperability should allow any user while at home or while roaming to be able to access any regional or tribal public safety network in order to reach any other users and any services at home network or at visited network.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 16

Layer 2 Connections supports the amendment to the definition proposed and feels that this definition of interoperability is best met by ensuring that common applications and services can be delivered to public safety agencies regardless of the type of network they use to connect. We acknowledge that the preferred end-state would be to have all agencies on a single, resilient, redundant, secure network that provides the appropriate coverage, quality and quantity of bandwidth for all eventualities. We caution that, even if this end-state were realistic and affordable, there will still be a significant migration period in which public safety agencies would be required to transition from the communications solutions they currently use to the new network. Additionally, once built, the 700 MHz public safety network is also a single point of failure, and during outages or times of congestion, there is still value in seamless failover to existing commercial networks used today.

[4] 47 C.F.R. § 90.7.

[5] *See* SAFECOM, http://www.safecomprogram.gov/SAFECOM/about/default.htm.

Chief Barnett offered similar recommendations recently[6]:

> "*…the public safety network must be able to expand its capacity to deal with extreme circumstances. For that reason, the FCC recommended that public safety be able to roam over to commercial networks with priority access…"*

We encourage the FCC to adopt rules that ensure that, to the greatest extent possible, applications and services are interoperable during this transition period and in emergencies where failover to commercial and private networks is required. Of critical importance will be the ability for agencies to utilize a hybrid solution consisting of the dedicated 700MHz Public Safety Broadband Network and whatever solution they use now or adopt during the migration period. By ensuring that any combination of applications and services can be made interoperable over any and all networks (wired as well as wireless) chosen by public safety agencies, the FCC will foster the exchange of voice and/or data between them while smoothing the difficult migration from a multitude of disparate networks towards the desired homogenous end-state.

EXTRACT – SECTION 17

As an initial matter, we consider the architecture of the public safety broadband network which is critical to ensure nationwide interoperability. We believe that the development of a uniform, nationwide architectural framework will promote a comprehensive understanding of interoperability and the steps that must be taken to achieve that objective. Below, we propose a set of high-level principles to guide development of the network in a manner that ensures interoperability. We seek comment on each of these principles. Do these principles capture all of the services and capabilities that the network must be capable of supporting to ensure interoperability? Do they reflect a realistic understanding of how the network will evolve over time?

[6] Statement of James Arden Barnett, Jr., Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission. "Keeping Us Safe: The Need for a Nationwide Public Safety Network." Presented before the U.S. Senate Committee on Commerce, Science, and Transportation. September 23, 2010.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 17

These principles do not capture all services and capabilities of which the network must be capable. Layer 2 Connections believes the architecture must also incorporate a means to seamlessly bridge existing commercial and private networks used today and in the future so that they act and behave as one with the 700 MHz public safety network. We understand that inter-RAT handoff is to currently expected to be addressed separately; we offer that it needs to be considered as a part of the architecture today.

We believe that the most significant problem faced by public safety is not the services and capabilities that must be supported by the 700MHz public safety network as it evolves but the support for the first iteration of these applications and services over a heterogeneous mix of the 700 MHz Public Safety Network and the various commercial and private networks currently being used by public safety agencies. We expect this period to last a considerable amount of time and be experienced by a significant number of public safety agencies.

Using Wide Area Network virtualization -- enabling multiple wide area networks to act and behave as one through a software and/or hardware solution operating at Layer 2 -- can accomplish this. We encourage the FCC to consider adopting this principle through the rulemaking process and codifying use of major capabilities of Wide Area Network Virtualization, such as "Make-before-break" Seamless Handoff and Network Bearer Bonding. These capabilities protect the situational awareness of the responder by protecting access to radio networks as well as protecting the data session as it transverses multiple networks

Additionally, we believe there is great benefit in extending Virtual Local Area Networks (VLANs) to mobile devices/units. By using VLANs in this way public safety agencies can extend the LAN data domains that support VoIP, GIS, Dispatch and other applications seamlessly to public safety users regardless of whether they are connected to the domain using a single network or disparate networks.

EXTRACT – SECTION 18.

18. Components of the Nationwide Network. The nationwide interoperable broadband network will comprise a set of interoperable, regional or tribal all-IP LTE networks operating in the public safety broadband spectrum; a nationwide IP backbone network; and additional network and service platforms at the national level.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 18

Layer 2 Connections believes that the definition should be expanded. The current definition describes a "network of networks" that only encompasses a patchwork of regional and tribal LTE networks. Layer 2 Connections believes this Nationwide Network should also have built-in resilience for users to seamlessly roam to existing 3G and 4G commercial and private networks. A user's data session should also be able to seamlessly roam from the Public Safety Broadband network to Wi-Fi and back to the Public Safety Broadband network. We expect in-building coverage will often be a challenge for the 700 MHz LTE network, and the ability to roam a data session to another network like Wi-Fi, can make the first responder safer and more productive – as he or she will have multiple paths available for secure connectivity.

EXTRACT – SECTION 20

20. As the LTE standard progresses, the network must become capable of supporting both mission-critical voice and data communications.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 20

We note that one essential feature of mission-critical voice and data communications is the ability to create, modify and manage its transfer between groups whose members often belong to multiple agencies. On broadband data networks this can be accomplished using broadcast and multicast techniques. Given our position that applications and services need to support interoperability over a combination of 700 MHz public safety and commercial/private networks, we believe it is essential that public safety agencies are provided with tools that facilitate the simultaneous delivery of mission critical voice and data communications over multiple networks. We believe that first responders should be able to rely on any combination of wired, wireless and satellite network to deliver them seamless and ubiquitous multicast services that don't break when moving from network to network or when bonding multiple networks together. Applications relaying on IP multicast -- often confined to private, localized networks -- should be made available to first responders on a wide area basis, offering them significant advantage and simplification of applications. This multicast ability could be delivered by a network overlay that adds functionality to networks that would not typically support multicast services. The ability to shape and prioritize multicast traffic over different networks is also very important.

EXTRACT – SECTION 27

27. The APCO Project 25 Steering Committee cautioned, however, that any implementation of "open standards" must accommodate the use of patented technologies that may be "the best technologies to support particular applications."

LAYER 2 CONNECTIONS' COMMENTS – SECTION 27

Like APCO, we recognize that many of the challenges posed by the adoption of the 700 MHz

Public Safety Network are beyond the scope of pure "open standards" specifications. We suggest an adaptation to the APCO language in the interest of serving first responders:

> "The APCO Project 25 Steering Committee cautioned, however, that any implementation of "open standards" must accommodate the use of patented *and/or mature* technologies that may be "the best technologies to support particular applications."

EXTRACT – SECTION 29

Further, we seek comments on the features of Release 9 and Release 10 that are necessary for applications such as real-time voice/video communications, location-based services, multicasting/broadcasting voice/video services, and other emergency preparedness related services.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 29

As previously mentioned we believe that such services need to be delivered reliably across legacy networks as well as the 700 MHz Public Safety Network. The most effective use case scenario is to allow data to flow over the most appropriate network for the type of data prioritizing traffic and shaping based on real time network performance metrics.

EXTRACT – SECTION 30

30. …We also seek comments on dual stack in order to support both IPv4 and IPv6.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 30

Given the likely extended period of migration from legacy communications networks to the 700MHz Public Safety Network, Layer 2 Connections believes that public safety agencies will need solutions that support both IPv4 and IPv6 networks for the foreseeable future. We believe that there are more flexible mechanisms than Dual Stack to support the features we describe in our response.

EXTRACT – SECTION 31

31. We also note that, although the prevalent tunneling protocol in LTE is GTP-based, a PMIP-based tunneling protocol has also been specified in 3GPP Release 8. This protocol is necessary in order to implement certain LTE interfaces. Supporting this protocol would require the adoption of an additional interface, namely Gxc (interface between SGW and PCRF when PMIP is used on S5 or S8). Should we require that public safety broadband networks adopt, in addition to the interfaces specified in the Third Report and Order, PMIP and the corresponding additional interface, Gxc? What are the potential costs and benefits of implementing such a requirement?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 31

Layer 2 Connections believes that whatever combination of fixed, wireless and satellite networks are used by first responders they must be able to support the features we describe in our response over all radio formats, including those specified in 3GPP.

EXTRACT – SECTIONS 35 AND 36

35. The 3GPP LTE standards set two categories of roaming: home-routed and local breakout. In home-routed roaming, the roamer's traffic is routed back to the home network to enable the use of home resources, while in local breakout roaming, the roamer utilizes the resources of the host network for desired services. The *Waiver Order* required the waiver recipients to support both methods.[7] We tentatively conclude that all public safety broadband networks should have the ability to support both categories of roaming. We seek comment on this tentative conclusion.

36. In the Plan, a recommendation was also made to require certain broadband commercial carriers to accommodate roaming by public safety broadband users. If, in a separate proceeding outside the scope of this item, we pursued such a requirement for commercial operators, are there any requirements that we should then impose on public safety broadband operators in this proceeding to ensure that their networks can interoperate with commercial broadband operators? Should the Commission take efforts in this proceeding to better enable public safety agencies to enter voluntary roaming agreements with commercial operators? If so, what should these incentives be?

[7] *See Waiver Order* at 5160 ¶ 45.

LAYER 2 CONNECTIONS' COMMENTS – SECTIONS 35 AND 36

We believe that, in addition to these two methods of roaming between networks of the same design, public safety agencies will benefit from being able to seamlessly roam between the 700 MHz Public Safety Network and commercial and private networks. This will significantly assist in agencies' migration to the 700 MHz network from their legacy systems. While we do not comment on the type of incentives that might be used to enable voluntary roaming with commercial operators, we do foresee that some of the networks will be technically and commercially cooperative to facilitating this roaming, some will be technically and/or commercially uncooperative and some will be between these extremes. We see success being measured by the ability to allow roaming on commercial and private networks regardless of their level of technical and commercial cooperation.

Given the increasingly critical nature of data services it will be important to ensure that the roaming between any and all networks is seamless (i.e., a "make-before-break" connection between networks). This is especially important given the rising prominence of real-time protocols that deliver voice and video communications. If the roaming is not seamless (i.e., "break-before-make"), then there will be a drop in communications while the transition from one network to another is achieved. This may result in hampered situational awareness and other undesirable consequences threatening the safety and productivity of the first responder.

In addition to delivering seamless roaming between networks we feel that it is important to allow the simultaneous use of both the 700 MHz Public Safety Network and one or many commercial and/or private networks. This allows agencies to benefit from increased resilience (no single point of failure), higher available bandwidth (through aggregation) and congestion avoidance (should preferred networks be overloaded).

Both the seamless roaming and network bonding features we describe should include network performance measurement that delivers quality of service over the multiple networks to accommodate VoIP, video and other priority-sensitive or real-time applications.

EXTRACT – SECTION 49

49. Additionally we seek comment, and raise the same questions as above, for the case where handover occurs between two eNodeBs from two different neighboring networks. This would be considered roaming. How is seamless handover possible in this situation?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 49

In addition to providing seamless handover between two eNodeBs from two different neighboring networks using LTE technology we recommend that the seamless handoff capability be extended to transitions between any and all nodes regardless of the network type in which they are deployed. Seamless handoff between nodes in two different physical (Layer 1) radio access types can be achieved by utilizing a common Layer 2 mobility layer.

EXTRACT – SECTION 50.

LTE supports mobility across the cellular network while maintaining a minimum level of performance, and supporting seamless handover. Do we need to set up support for a minimum speed (in mph) for mobility and seamless handover while within a regional or tribal network? Similarly, do we need to set up support for a minimum speed for mobility and seamless handover while crossing neighboring networks (roaming)?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 50

Layer 2 Connections advocates that the speed for mobility and seamless handover should be set so that there is no delay in roaming to neighboring networks that can be discernable by public safety users utilizing real-time voice and video applications to perform their mission-critical operations.

EXTRACT – SECTION 55

55. Does VPN access imply client-based VPNs and if, so, is any network support required? If the network does not allow all protocols, what kinds of VPN protocols should be allowed, such as IPSec, PPTP or L2TP? Does this application imply a requirement for the network to operate such a server and how should it be identified?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 55

Layer 2 Connections' believes that it is in the interests of public safety agencies to allow all types of VPN to be used over the 700 MHz Public Safety Network. We believe that a wide area virtualization layer should provide VPN and encryption but should also be able to transparently provide a transport layer for any other VPN solution and in doing so enable it to have seamless mobility across changing radio network layers.

EXTRACT – SECTION 57

57. The Commission anticipates that an all-IP wireless broadband LTE network will enable public safety agencies to select from a diverse array of evolving applications and services to support their communications needs, including real-time voice and video communications. We seek comment on how we can promote the interoperability of key applications that are not included among the set of common applications that all public safety networks will be required to support. What interfaces impact application interoperability?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 57

We believe that wide area network virtualization can deliver the interoperability of key applications across all media and network types by promoting seamless mobility between networks and bandwidth bonding on multiple networks simultaneously regardless of their type.

EXTRACT – SECTION 58

58. We seek comment on how to address the interconnection of existing narrowband public safety networks (both voice and data) in multiple bands (Legacy Networks) with the public safety broadband network in the absence of the Public/Private Partnership called for in the *Second Report and Order*….Can these gateways between Legacy and public safety broadband networks offer both voice and data services?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 58

If legacy networks are interconnected and used in the transition period while the 700 MHz network is being implemented then we urge the FCC to leverage the use of wide area network virtualization technology to ensure that data roaming between these networks is seamless and that the networks can be bonded together to provide greater resilience and bandwidth when needed. Use of wide area virtualization technology should accommodate legacy networks today and be "future proof" for new networks yet to come.

EXTRACT – SECTION 59

59. We [the FCC] recognize the importance of ensuring that public safety broadband networks have adequate capacity, spectral efficiency, QoS and overall performance to achieve nationwide interoperability. Spectrum is a valuable public resource and the Commission is committed to ensuring that this resource is used efficiently. Moreover, we believe that imposing baseline operability requirements on public safety broadband networks ensures that disparate networks are capable of interoperating. We tentatively conclude that in order to ensure baseline operability and to ensure the efficient use of the radio frequency resource, it is appropriate to adopt performance requirements for public safety broadband networks. We seek comment on

this tentative conclusion.

LAYER 2 CONNECTIONS’ COMMENTS – SECTION 59

We agree that spectrum is a valuable public resource and that baseline operability requirements for public safety broadband networks will ensure disparate networks are capable of interoperating. We strongly urge the commission to extend the scope of these operability requirements to include networks beyond the 700 MHz Public Safety network with other radio interfaces. Interoperability between networks with disparate radio interfaces can be achieved using Layer 2 wide area network virtualization.

EXTRACT – SECTION 60

60. If public safety networks are not built with baseline operability requirements and high spectral efficiency, both operability and interoperability may fail in an emergency when the demand for communications is greatest.

LAYER 2 CONNECTIONS’ COMMENTS – SECTION 60

We observe that networks will fail even with well-established baseline operability requirements and high spectral efficiency. The best way to handle this is to make worst case assumptions that networks will fail and mitigate this failure with as much redundancy as possible. By allowing public safety agencies to seamless failover to commercial and private networks and by giving them the ability to bond these disparate networks together for additional bandwidth the FCC will ensure maximum availability and maximum usage of spectrum resources.

EXTRACT – SECTION 70

70. “It is critical that public safety have available to it a resilient and reliable public safety broadband network.”

LAYER 2 CONNECTIONS' COMMENTS – SECTION 70

In addition to building resilience and reliability into the 700 MHz Public Safety Network in the manner described we encourage the FCC to extend the resilience and reliability of public safety communications by utilizing commercial and private networks. Layer 2 Connections' viewpoint is that the less common components that these alternative networks share with each other, the more resilience and reliability they can deliver to public safety agencies.

In addition, roaming between the future 700 MHz Public Safety network and commercial wireless networks is consistent with direction previously given by the Public Safety and Homeland Security Bureau[8]:

> *"…the public safety network must be able to expand its capacity to deal with extreme circumstances. For that reason, the FCC recommended that public safety be able to roam over to commercial networks with priority access…"*

EXTRACT – SECTION 72

72. One approach we can take is to require that the public safety broadband networks cover a certain population or geographic benchmark. Such requirements could impose costs on public safety but could ensure that an increased percentage of the nation benefits from the public safety broadband network and hence, is interoperable. Is this an appropriate requirement to impose on public safety? If so, what percentage of population-based or geographic coverage benchmark should we adopt for the public safety broadband network? Should coverage requirements be implemented over a fifteen-year period? If a fifteen-year period were implemented, should the Commission require that the network achieve 40 percent coverage within four years, 75 percent within ten years and 99 percent within fifteen years?

[8] Statement of James Arden Barnett, Jr., Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission. "Keeping Us Safe: The Need for a Nationwide Public Safety Network." Presented before the U.S. Senate Committee on Commerce, Science, and Transportation. September 23, 2010.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 72

Regardless of the coverage requirements that get adopted we anticipate that the 700 MHz Public Safety Network will have to co-exist with multiple legacy commercial and private networks for a considerable period of time. We believe it is therefore essential that the FCC take steps to ensure that public safety agencies are provided tools that allow them to fully integrate legacy and public safety broadband networks together to achieve the highest possible coverage and availability. One suggestion is that a cost benefit analysis be performed using existing and planned build out of private and public networks (including satellite and wire line) to establish a realistic and affordable plan. The goal should be to utilize all available network capacity, as may be needed in an emergency. This might be achieved, for instance, by establishing tax credits for companies willing to make their company networks part of the national network available in times of emergency. This would allow public safety agencies to utilize what already exists and would allow public safety broadband network operators to plan their future buildout accordingly.

EXTRACT – SECTION 85 (including reference 97)

85. In an effort to enhance the utility of the public safety broadband networks recently authorized by early build out waivers[9] and to foster the continued evolution towards a national public safety broadband network in the 700 MHz band, we now seek to establish technical requirements and a regulatory framework to govern public safety roaming on 700 MHz public safety broadband networks (intra-system roaming).[10] We expect that this framework will enhance interoperability in both day-to-day and emergency situations.

Reference 97 - Roaming for 700 MHz public safety users can occur in two circumstances: (1) when a public safety user travels to another region and logs into another public safety network using the same public safety band in 700 MHz spectrum, or (2) when a public safety user either travelling to another region or within his or her own region faces a situation in which either there is no coverage for public safety band or there is not sufficient capacity at the time, and hence, the user roams on to a commercial band. We adopt the nomenclature used in the NPSTC BBTF Report, which terms the first circumstance "intra-system roaming"—where public safety roams into another public safety network within the same band. The second circumstance is termed

[9] *See Waiver Order*.

[10] See Reference 97.

"inter-system roaming"—where public safety roams into commercial networks in another band. The scope of this *Fourth Further Notice* is limited to the issues concerning the intra-system roaming, and the issues concerning the inter-system roaming are to be addressed separately.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 85

Layer 2 Connections understands that the issues of inter-system roaming will be addressed separately. Please note that the "Make-Before-Break" Seamless Handoff capabilities described throughout our commentary affect both intra-system roaming and inter-system roaming.

EXTRACT – SECTION 93

Broadband technologies can advance public safety and homeland security by improving the operability, interoperability, and usability of public safety communications. In particular, public safety applications could seamlessly be available to all users at home and while roaming during day to day tasks as well as in times of emergency. Recognizing these benefits of broadband technologies to public safety, we have tentatively concluded in Section A.16 above to adopt five common applications that must be fully supported by each public safety broadband network. In order to further advance interoperability across networks, we extend this tentative conclusion here by proposing that all networks support this same set of applications for the purpose of roaming. Therefore, we tentatively conclude that public safety broadband networks must support the following five applications to intra-system roamers: (1) Internet access; (2) VPN access to any authorized site and to home networks; (3) a status or information "homepage;" (4) access to responders under the Incident Command System; (5) and field-based server applications. We seek comment on this tentative conclusion. Are there additional applications that should be supported for roaming purposes?

LAYER 2 CONNECTIONS – SECTION 93

Layer 2 Connections suggests that the FCC should mandate the support of IP Multicast. This will facilitate support for ubiquitous voice and video communications to a range of first responders who may require to communicate using the same multicast-enable applications and services but may often be connected to those applications and services via disparate network technologies each of which may be managed by a different identity and/or authorization authority.

EXTRACT – SECTION 122

122. *Multiple Mode Support*: As LTE networks are built out for public safety and commercial usage, multiple mode devices may provide additional coverage with 2G/3G support.124 Commercial multiple mode LTE devices are type approved to support either GPRS/EDGE/WCDMA/HSPA platform or CDMA/EVDO platform in various frequency bands. What factors should public safety entities consider when selecting LTE devices? Further, given the coverage limitations of terrestrial wireless networks, what are the possibilities of adding satellite capability to public safety LTE device? Does satellite capability favor any particular 2G/3G/4G technology platform? What, if any, action should the Commission take here?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 122

Layer 2 Connections believes that it will be far less costly for each public safety agency to purchase a number of single mode devices based mainly on "Commercial Off The Shelf" products than to source more specialized multi-mode devices. Multi-mode devices tend to be expensive to manufacturer, and are also limited in that normally only one radio technology may be used at a time. The benefits of having multiple devices include: resilience through redundancy, simultaneous multi-mode connectivity (allows bonding of different network types at the same time), make-before-break seamless roaming (multiple interfaces up at the same time), multiple network monitoring (allows informed bandwidth utilization), standard form factors (many multi-mode chipsets require too much space to fit on industry standard PCI Express Card form factor). We believe that effective connection management can deliver far greater system flexibility with minimal downsides. We believe our comments about Multiple Mode devices also hold true for Multiple Band devices.

EXTRACT – SECTION 126

126. Finally, what other approaches may be used to further support the in-building communication needs of public safety users?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 126

We believe that the FCC should adopt rules that allow public safety agencies maximum flexibility as to the modes and bands of wireless access technologies available for in-building coverage. Rules should ensure effective management of the "Make-Before-Break" Seamless Roaming and Network Bearer Bonding of in-building systems -- whatever type they may be. In this way, users can benefit from the ability to roam from the Public Safety Broadband Network to, as an example, an in-building public WiFi network, and seamlessly roam back to the Public Safety Broadband Network – without loss of connectivity. The user could also bond the network bearers together. In either case, the user stays connected, leveraging both new and existing infrastructure. Real-time protocols such as VoIP and Video transition without interruption. And cost of network build is also reduced by leveraging existing investments. These are a few ways in which mandating "Make-Before-Break" Seamless Handoff and Network Bearer Bonding as capabilities can improve the safety and productivity of first responders.

EXTRACT – SECTION 127

The Plan recommends that public safety agencies use deployable equipment, during natural disasters and in other circumstances,[11] to supplement their existing coverage and capacity and to provide a source of redundancy.[12] This equipment may include cells on wheels (COWs) and cells on light trucks (COLTS), which may be configured either as stand-alone base stations[13] or as repeater stations. COWs and COLTs may be deployed during an emergency, for example, to temporarily replace damaged sites or to support surges in traffic.[14] They can also support communications during events that occur at a cell edge, where coverage and capacity may be marginal. In addition to COWs and COLTs, signal repeaters located within public safety vehicles can be used to relay signals from portable user equipment back to a base station.[15]

[11] These deployable assets could also be used for supplementing in-building coverage.

[12] *See* National Broadband Plan at 318, Exhibit 16-B: National Safety Network and Solutions; *see also* Cost Model Paper at 3.

[13] Under the 3GPP LTE standard, base stations are referred to as "Enhanced NodeBs", or "eNodeBs".

[14] In mobile data networks higher signal levels above noise and interference level are proportional to available data rates. In addition, introducing bandwidth in a given area allows the introduction of the corresponding capacity to users in that area.

[15] *See* Cost Model Paper at app. A.

LAYER 2 CONNECTIONS' COMMENTS – SECTION 127

We believe that the FCC should adopt rules that allow public safety agencies maximum flexibility as to the modes and bands of wireless access technologies available deployable equipment used during natural disasters. Rules should ensure effective management of "Make-Before-Break" Seamless Handoff and Network Bearer Bonding of deployable systems whatever type they may be.

EXTRACT – SECTION 131

We [the FCC] believe that it is critical that public safety community has the broadband tools it requires to keep America safe. Accordingly, we seek comment on what can be done to ensure that the 4.9 GHz band networks can complement the 700 MHz broadband networks. What can be done to increase this compliment?

LAYER 2 CONNECTIONS' COMMENTS – SECTION 131

We believe that the FCC should adopt rules that allow public safety agencies maximum flexibility as to how they use 4.9 GHz band networks. Rules should ensure effective management of "Make-Before-Break" Seamless Handoff and Network Bearer Bonding of 4.9 GHz and 700 MHz networks.

CONCLUSION

Layer 2 Connections urges the FCC to consider several important areas in its rulemaking.

- There is a need for rules that address the transition from commercial and private networks used by public safety agencies today to emerging 700 MHz Public Safety networks. These same rules should also affect seamless failover of data sessions from the 700 MHz network to existing commercial and private networks available during times of emergency, congestion or out-of-coverage challenges.

- In emergency situations public safety agencies may need to extend the coverage and capacity of their communications networks while also delivering more resilience. Making use of multiple networks at the same time is critical to their safety and productivity.
- Regardless of whether a single network or "network-of networks" approach is taken for the 700 MHz Public Safety Network we anticipate that a variety of legacy networks will need to be supported. Layer 2 Connections suggests that applications and services need to be network-agnostic placing public safety agencies in full control of how current and future networks are used for what purpose and by whom.

Layer 2 Connections' three specific requests of the FCC for consideration in rulemaking are offered in the public interest of improving the safety and productivity of our nation's first responders:

1. The FCC should extend the concept of the "network of networks" from referring to the combination of all Regional and Tribal 700 MHz Public Safety Networks to encompass networks of all types – regardless of mode or band.

2. The FCC define and mandate that roaming handoff – whether intra-system or inter-system – be defined explicitly as requiring a "Make-Before-Break" Seamless Handoff in order to ensure that critical applications (especially real-time applications such as VoIP and Video) do not suffer an interruption or delay during transition of network.

Such capabilities can also expand coverage of the National 700 MHz Public Safety Broadband network into in-building locations by leveraging existing WiFi and other assets.

3. The FCC mandate that the capability of Network Bearer Bonding – enabling the combined bandwidth of multiple similar and/or dissimilar networks to be utilized for the same data session simultaneously – improving resilience and providing additional capacity outside of the 700 MHz Public Safety Broadband Network. This capability expands first responder options for connectivity to critical applications, especially in times of outage and congestion – which are common to networks in times of emergency.

Layer 2 Connections is a small, woman-owned business based in North Carolina with experience serving the public safety community with mission-critical voice and data communications.

If you have any questions or comments regarding these comments, please do not hesitate to contact any of the Layer 2 Connections principals below at 919.300.7733 or via email as listed.

Sincerely,

/s/ Pascal de Hesselle

Pascal de Hesselle
Principal
Layer 2 Connections, LLC
13016 Eastfield Road, Suite 280
Huntersville, NC 28078
pascal@layer2connections.com

/s/ Marc Le Maitre

Marc Le Maitre
Principal
Layer 2 Connections, LLC
121 Bridgette Place
Leesburg, VA
marc@layer2connections.com

/s/ Susan Nelson

Susan Nelson
Managing Principal
Layer 2 Connections, LLC
104R NC Hwy 54, Suite 327
Carrboro, NC 27510
susan@layer2connections.com

CC (via email):

Jamie.Barnett@fcc.gov
Jennifer.Manner@fcc.gov
David.Furth@fcc.gov
Genaro.Fullano@fcc.gov
Brian.Hurley@fcc.gov
William.Lane@fcc.gov
Richard.Lee@fcc.gov
Yoon.Chang@fcc.gov